



# CYBERSECURITY SALES MASTERCLASS

---

*The Pre-Sale Process*

- Our Role
- Assumptions
- Questions to ask
- Talk tracks
- Starting the conversation
- Knowing the “NO”
- Talk Tracks
- Steps to success

# TODAY'S DISCUSSIONS

# LET'S START AT THE BEGINNING

---

A Jack of all trades is a master of none

Today

We will embark on our journey toward becoming a  
master of SOME!

# EDUCATION IS OUR JOB

---

Cybersecurity is complicated but getting started doesn't have to be

## COMMENT IN THE CHAT

How many of you think your customers know about cybersecurity?

## BE CAREFUL HERE

**Assuming your prospect has a knowledge of your program or service is a danger ground.**

- 51% of small businesses think it's unlikely or very unlikely that they'd be targeted for a cyber attack.
- 71% of those who have never experienced a breach thought that the potential damage to their reputation wasn't an important consideration.

If you assume your prospects place the same importance on cybersecurity as you do, you could make the mistake of passing over the real benefits of your services or program.

After all, you can't sell the solution to a problem your prospect doesn't believe they have.

## BASIC QUESTIONS

- How are you adopting work from home?
  - Are you allowing end-users to use their personal devices ?
- What are your top 3 security concerns?
  - Most companies are worried about being breached and losing data does that concern you?
  - Many companies we work with have implemented a multifactor solution into their company, have you or have you thought about it?
  - The biggest risk that a company has is their employees, do you have any idea of your employee's cyber hygiene or risk profile?

## GOAL

Our goal here is to get them talking and see what their take is on cybersecurity and to gauge how much work it will take to get them to take the steps toward success.





**WE NEED TO MAKE THEM  
FEEL COMFORTABLE WITH  
CHANGE**



# STARTING THE CONVERSATION

- Resources
- Webinars
- Email Communications
  - As they come out
  - Monthly



What are some of the ways that you are engaging with your customers to educate them?

## COMMENT IN THE CHAT

What are the most common objections or “NO’s” you have received talking with your customers about cybersecurity services?



Send us your best objections so in the next class we can discuss objection handling. Email: [Hello@hacware.com](mailto:Hello@hacware.com)

## KNOWING THE “NO” IS IMPORTANT

- I don't have money for cybersecurity
- It won't happen to me
- We already have protection that covers us and is adequate
- No one is interested in my data
- I'll wait until my insurance requires us to do something
- We have been in business for years and never had a problem
- I don't see the reason that I need to pay for more since you take care of everything.

# CUSTOMER TALK TRACKS FOR THE MODERN MSP

- What cyber threats concern you the most?
- Are your information security and business priorities aligned?
- Do we know where our data is and how it is protected?
- Are your employees being appropriately trained on cybersecurity?
- Do you know how to respond in a cybersecurity emergency?
- Do your documented policies match what is actually happening in your practice?



This resource will be sent to you after the session

# THE BUSINESS CONVERSATION

- **Insufficient security measures:** 45% say that their processes are ineffective at mitigating attacks.
- **Frequency of attacks:** 66% have experienced a cyber attack in the past 12 months.
- **Background of attacks:** 69% say that cyber attacks are becoming more targeted.

## The most common types of attacks on small businesses include:

- **Phishing/Social Engineering:** 57%
- **Compromised/Stolen Devices:** 33%
- **Credential Theft:** 30%

# TOP DISCUSSION TOPICS

The Reason	The Top 5	Security	The Money	Social Responsibility
There are 30 million SMB in the USA and over 66% of all SMBs had at least 1 incident between 2018-2021.	<ul style="list-style-type: none"><li>• Cyber threats</li><li>• Identity theft</li><li>• Data breach</li><li>• Security &amp; Business alignment</li><li>• Cyber security Education</li></ul>	Its no longer an option it's a requirement for modern businesses and its our job to protect our employees and its customers.	Access to someone's entire online identity is worth roughly \$1,000 for 2022.	Social responsibility is an ethical framework in which an individual is obligated to work and cooperate with other individuals and organizations for the benefit of the community that will inherit the world that individual leaves behind.

# A PROCESS FOR PRESALES SUCCESS



## Step 1 ●

Define your strategy and ensure your contracts and sales materials support your new offering



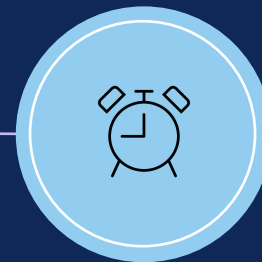
## Step 2 ●

Prepare emails that are relevant to cybersecurity and begin sending them outreach week/month



## Step 3 ●

Launch customer facing lunch and learns/webinar series to educate your customers



## Step 4 ●

Take your time, not everyone will come running. Remember they will gain trust over time.



## Step 5 ●

Once you have a customer ready to commit, make sure you execute and hold yourself accountable to mutual success.



# RESOURCES

## Customer Talk Tracks

- Will be sent out via email after the meeting.

## Slide Deck

- Will be sent out via email after the meeting.

## Hack Assessment

- <https://resources.hacware.com/hack-assessment/>

## Quick Links to Valuable Data

- <https://connect.comptia.org/content/research/it-industry-trends-analysis>
- <https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/>

# CONNECT WITH US

---

Follow us:

[Linkedin.com/company/hacware/](https://www.linkedin.com/company/hacware/)

Join our LinkedIn Group where we will continue this conversation.

<https://www.linkedin.com/groups/14159275/>